(19) Bundesrepublik Deutschland
Deutsches Patent- und Markenamt

(10) **DE 102 35 819 A1** 2004.02.26

(12) # Offenlegungsschrift

(21) Aktenzeichen: **102 35 819.2**
(22) Anmeldetag: **05.08.2002**
(43) Offenlegungstag: **26.02.2004**

(51) Int Cl.[7]: **G06F 15/163**

(71) Anmelder:
Schneider, Utz, 13409 Berlin, DE; Mauszewski, Dirk, 14193 Berlin, DE

(74) Vertreter:
Grape & Schwarzensteiner, 80331 München

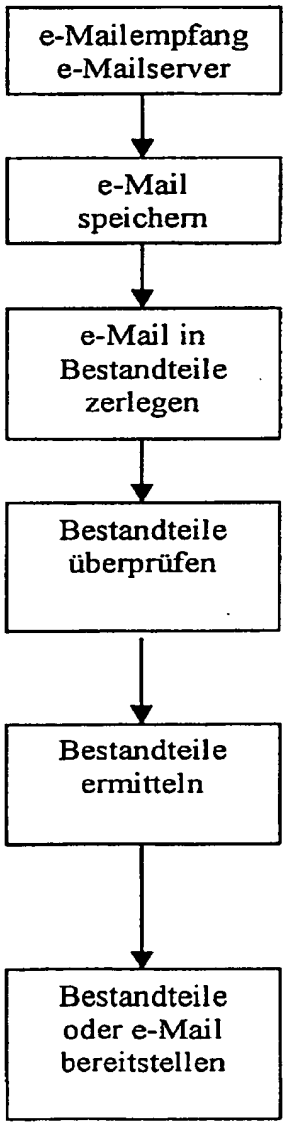
(72) Erfinder:
Schneider, Utz, 13409 Berlin, DE

Prüfungsantrag gemäß § 44 PatG ist gestellt.

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Bezeichnung: **Verfahren und Anordnung zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen sowie deren Verwendung**

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren und eine Anordnung zum Blockieren von an einem Benutzer gesendeten Daten und/oder Informationen und/oder Signalen elektronischer Medien, insbesondere von aktiven E-Mail-Inhalten, aus einem elektronischen Datennetz, insbesondere aus dem Internet oder sonstigem Intranet, umfassend eine Einrichtung zum Empfangen der an den Benutzer gesendeten Daten und/oder Informationen und/oder Signale von einer Datenverarbeitungseinrichtung, insbesondere einem Server, aus dem elektronischen Datennetz, eine Einrichtung zum Speichern der empfangenen Daten und/oder Informationen und/oder Signale in der Datenverarbeitungseinrichtung, eine Einrichtung zum Zerlegen der gespeicherten Daten und/oder Informationen und/oder Signale in deren Bestandteile, eine Einrichtung zum Überprüfen der Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale auf aktiven Inhalt, eine Einrichtung zum Ermitteln der Bestandteile der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt, und eine Einrichtung zum Bereitstellen der Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt auf der Datenverarbeitungseinrichtung zum gezielten Abruf durch den Benutzer, sowie deren Verwendung.



Beschreibung

[0001] Die Erfindung betrifft ein Verfahren und eine Anordnung zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen elektronischer Medien sowie deren Verwendung.

Stand der Technik

[0002] Es hat sich in der Praxis herausgestellt, dass die Verbreitung von Viren mit zunehmender Verwendung elektronischer Medien zur Kommunikation zwischen Benutzern untereinander ständig anwächst. Ein häufiger Verbreitungsweg für Viren ist dabei die Verwendung von e-Mails über ein elektronisches Datennetz, wie dem Internet oder sonstigem Intranet. Eine e-Mail besteht dabei aus einer einzelnen physikalischen Datei, die mehrere logische Abschnitte umfasst, welche wiederum eine einzelne Datei bzw. einen sogenannten Dateianhang oder andere Informationen beinhaltet. Die als e-Mail versandte, physikalische Datei wird von sogenannten Standard-Mail-Clients von einem Server, zum Beispiel einem Mail-Server, abgerufen und dem Benutzer in Form der einzelnen logischen Abschnitte, insbesondere als Dateianhänge etc., separat zur Verfügung gestellt. Die mittels e-Mail versendeten Viren befinden sich selbst in den mitgesendeten Dateianhängen und werden bei deren Ausführung, beispielsweise einer Datei EXE-Format, oder Sichtung, beispielsweise einer Datei im DOC-Format, ausgeführt. Eines der wesentlichen Probleme besteht darin, dass eine solche Ausführung oder Sichtung von Seiten des Benutzers unbeabsichtigt erfolgen kann, indem der Typ des jeweiligen Dateianhangs verschleiert wird. Der Benutzer, welcher eine e-Mail-Datei erhält, ist sich insoweit nicht bewusst, dass er eine e-Mail mit einer Datei mit aktivem, möglicherweise potentiell gefährlichem e-Mail-Inhalt erhalten hat. Zur Ausführung oder Sichtung der e-Mail ist der Benutzer daher gezwungen, deren Dateien bzw. Dateianhänge zu öffnen und damit zu aktivieren. Das Risiko, mit der Ausführung oder Sichtung der e-Mail zugleich Viren aufzurufen, ist für technisch weniger versierte Benutzer zudem noch ungleich höher, da diese entsprechende Informationen zur Beurteilung des Typs der Datei, Besonderheiten der e-Mail etc., nicht besitzen. Zusätzlich können Viren in e-Mails, welche HTML-formatiert sind, enthalten sein, die sofort bei der Sichtung des e-Mails aktiviert werden.

[0003] Um eine unwillkürliche und unbeabsichtigte Ausführung oder Sichtung von aktiven e-Mail-Inhalten, wie zum Beispiel Programmen, Skripten und/oder Virenprogrammen, zu verhindern, werden derzeit Antivirenprogramme eingesetzt. Diese auf Muster und/oder Erkennung mittels heuristischer Verfahren basierenden Antivirenprogramme schützen allerdings nur gegen bekannte Viren und müssen täglich aktualisiert werden. Mithin gelingt es neuen und damit für die Antivirenprogramme unbekannten, in jüngster Zeit zugleich sich massiv verbreitenden Viren, sich nach unbeabsichtigter Ausführung oder Sichtung durch den Benutzer innerhalb weniger Tage oder auch nur Stunden weltweit zu verbreiten. Die Folge davon ist ein zum Teil erheblicher Schaden in Abhängigkeit des jeweiligen sogenannten Payloads, d.h. von den im Virus enthaltenen Schadensroutinen, zumindest aber eine Beeinträchtigung des die e-Mail empfangenden Systems in dessen Leistung. Darüber hinaus ist ein Schutz mittels Antivirenprogrammen in Fällen ausgeschlossen, in welchen die Viren speziell zu Sabotage- oder Spionagezwecken gefertigt wurden, welche sich nicht weiter verbreiten und insoweit den Herstellern von Antivirenprogrammen weitgehend unbekannt bleiben.

Aufgabenstellung

[0004] Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Anordnung zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen elektronischer Medien, insbesondere von aktiven e-Mail-Inhalten, aus einem elektronischen Datennetz zur Verfügung zu stellen, mit welchem bzw. welcher sich die obigen Nachteile verhindern lassen, welches bzw. welche mithin konstruktiv einfach, zugleich ausgesprochen zuverlässig sowie besonders kostengünstig ist, sowie deren Verwendung bereitzustellen.

[0005] Diese Aufgabe wird in verfahrenstechnischer Hinsicht auf überraschend einfache Weise durch die Merkmale des Anspruchs 1 gelöst.

[0006] Demnach ist durch die Ausgestaltung des erfindungsgemäßen Verfahrens zum Blockieren von an einen Benutzer gesendeten Daten, Datenzellen oder Datenpaketen und/oder Informationen und/oder Signalen elektronischer Medien, insbesondere von aktiven e-Mail-Inhalten, aus einem elektronischen Datennetz, insbesondere aus dem Internet oder sonstigem Intranet, umfassend folgende Schritte:

a) Empfangen der an den Benutzer gesendeten Daten und/oder Informationen und/oder Signale von einer Datenverarbeitungseinrichtung, insbesondere einem Server, aus dem elektronischen Datennetz,

b) Speichern der empfangenen Daten und/oder Informationen und/oder Signale aus Schritt a) in der Datenverarbeitungseinrichtung,

c) Zerlegen der gespeicherten Daten und/oder Informationen und/oder Signale aus Schritt b) in deren Bestandteile,

d) Überprüfen der Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale aus Schritt c) auf aktiven Inhalt,
e) Ermitteln der Bestandteile der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt, und
f) Bereitstellen der Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt aus Schritt d) und e) auf der Datenverarbeitungseinrichtung zum gezielten Abruf durch den Benutzer,

[0007] ein Verfahren bereitgestellt, mit welchem sich auf sehr einfache Weise eine unwillkürliche und unbeabsichtigte Aktivierung von e-Mails mit aktiven schädlichen e-Mail-Inhalten verhindern, zumindest aber wesentlich erschweren lässt. Der Benutzer und damit der Empfänger der e-Mail kann dabei ungefährdet an deren Informationsgehalt gelangen. Zugleich ist allerdings der Zugang zu möglicherweise gefährlichen Bestandteilen der e-Mail oder sogar der gesamten e-Mail im Original möglich. Insgesamt wird durch das erfindungsgemäße Verfahren verhindert, dass Viren nach dem Empfang einer e-Mail mittels des beim Benutzer bzw. Empfänger vorhandenen e-Mail-Inhalts in das System des Benutzers gelangt, ohne dass der eigentliche Informationsgehalt der e-Mail teilweise oder sogar vollständig verloren geht. Damit einhergehend lässt sich zugleich ein ausgesprochen kostengünstiges Verfahren zum Blockieren der an den Benutzer gesendeten Daten, Datenzellen oder Datenpaketen und/oder Informationen und/oder Signalen elektronischer Medien erhalten.
[0008] Weitere vorteilhafte Einzelheiten des erfindungsgemäßen Verfahrens sind in den Ansprüchen 2 bis 14 beschrieben.
[0009] Vorteilhafterweise werden die gespeicherten Daten und/oder Informationen und/oder Signale in deren kleinstmögliche Bestandteile zerlegt. Auf diese Weise ist sichergestellt, dass tatsächlich auch sämtliche Daten und/oder Informationen und/oder Signale einer Überprüfung unterzogen werden. Zugleich lässt sich damit eine weitestgehende Trennung von Daten und/oder Informationen und/oder Signalen ohne aktiven Inhalt einerseits und mit aktivem Inhalt andererseits erreichen. Der auszuführende bzw. zu sichtende Informationsgehalt kann daher in eine ungefährliche Kategorie und eine gefährliche Kategorie weiter optimiert eingeordnet werden.
[0010] Weiterhin liegt es im Rahmen der Erfindung nach Anspruch 3, dass die Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale vor deren Überprüfung klassifiziert und (zwischen-)gespeichert werden.
[0011] Von besonderer Bedeutung für eine einfache, zuverlässige und umfassende Überprüfung der Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale sind die Merkmale des Anspruchs 4, wonach die Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale wenigstens teilweise, vorzugsweise sämtlich, in Bestandteile ohne aktiven Inhalt konvertiert werden.
[0012] In diesem Zusammenhang ist erfindungsgemäß vorgesehen, dass die Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale nach Anspruch 5 automatisch oder alternativ nach Anspruch 6 auf (individuelle) Anforderung in Bestandteile ohne aktiven Inhalt konvertiert werden.
[0013] Von ausgesprochen großem Interesse für einen sicheren, zugleich zuverlässigen und umfassenden Abruf des Informationsgehaltes einer e-Mail sind weiterhin die Maßnahmen des Anspruchs 7. Demnach werden die nicht-konvertierbaren Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale mit aktivem Inhalt ermittelt und besonders gekennzeichnet. Der Benutzer wird insoweit über den Typ und die möglicherweise potentiell vorhandene Gefährlichkeit einzelner Bestandteile der e-Mail oder sogar der gesamten e-Mail informiert, und zwar unabhängig von dem eingesetzten lokalen Programm der e-Mail.
[0014] Weiterhin liegt es nach Anspruch 8 im Rahmen der Erfindung, dass die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt zusammen mit den Bestandteilen der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt auf der Datenverarbeitungseinrichtung zum Abruf durch den Benutzer bereitgestellt werden. Alternativ dazu ist erfindungsgemäß nach Anspruch 9 vorgesehen, die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt getrennt von den Bestandteilen der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt auf der Datenverarbeitungseinrichtung zum Abruf durch den Benutzer bereitzustellen. Entsprechend der Maßnahmen der Ansprüche 8 und 9 ist so in jedem Fall sichergestellt, dass der Benutzer vollumfänglich den Informationsgehalt der e-Mail Kenntnis erlangen kann. Ob dabei die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt zusammen mit bzw. getrennt von denjenigen mit aktivem Inhalt bereitgestellt werden, hängt lediglich von der auszuwählenden bzw. gewünschten Sicherheitsanforderung ab. Die Sicherheitsanforderung kann dabei entweder von dem Provider und kumulativ oder alternativ von dem Benutzer selbst beliebig vorbestimmt bzw. festgelegt werden.
[0015] Weiterhin liegt es nach Anspruch 10 im Rahmen der Erfindung, dass die auf der Datenverarbeitungseinrichtung bereitgestellten Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt von dem Benutzer unmittelbar abgerufen werden.
[0016] Einer weiteren Erhöhung der Sicherheit beim Abruf des gesamten Informationsgehaltes einer e-Mail dienen des Weiteren die Maßnahmen des Anspruchs 11, wonach die auf der Datenverarbeitungseinrichtung bereitgestellten Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder

mit aktivem Inhalt von dem Benutzer mittelbar abgerufen werden. Einer versehentlichen Ausführung oder Sichtung von aktiven e-Mail-Inhalten ist somit entgegengewirkt, zumindest für den Benutzer erschwert, da ein gezielter Abruf der Bestandteile der Daten und/oder Informationen und/oder Signale in jedem Fall einer weiteren Anweisung bzw. Instruktion von Seiten des Benutzers bedarf.

[0017] In diesem Zusammenhang ist es besonders vorteilhaft, dass die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt nach Anspruch 12 durch gesondertes Aufrufen eines Links im elektronischen Datennetz und/oder alternativ dazu nach Anspruch 13 durch gesondertes Absenden einer Bestätigung zum Herunterladen über das elektronische Datennetz auf der Datenverarbeitungseinrichtung zum Abruf durch den Benutzer bereitgestellt werden.

[0018] Des Weiteren wird diese Aufgabe in vorrichtungstechnischer Hinsicht durch die Merkmale des Anspruchs 14 gelöst.

[0019] Demnach umfasst die erfindungsgemäße Anordnung zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen elektronischer Medien, insbesondere von aktiven e-Mail-Inhalten, aus einem elektronischen Datennetz, insbesondere aus dem Internet oder sonstigem Intranet, eine Einrichtung zum Empfangen der an den Benutzer gesendeten Daten und/oder Informationen und/oder Signale von einer Datenverarbeitungseinrichtung, insbesondere einem Server, aus dem elektronischen Datennetz, eine Einrichtung zum Speichern der empfangenen Daten und/oder Informationen und/oder Signale in der Datenverarbeitungseinrichtung, eine Einrichtung zum Zerlegen der gespeicherten Daten und/oder Informationen und/oder Signale in deren Bestandteile, eine Einrichtung zum Überprüfen der Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale auf aktiven Inhalt, eine Einrichtung zum Ermitteln der Bestandteile der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt, und eine Einrichtung zum Bereitstellen der Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt auf der Datenverarbeitungseinrichtung zum gezielten Abruf durch den Benutzer. Durch eine solche Ausgestaltung der Anordnung nach der Erfindung ist es auf besonders einfache, zugleich aber sehr zuverlässige Weise möglich, eine unwillkürliche und unbeabsichtigte Ausführung oder Sichtung aktiver e-Mail-Inhalte zu verhindern bzw. wenigstens zu erschweren. Damit einhergehend lassen sich auch die Kosten, die nicht zuletzt durch Schäden oder sonstige Beeinträchtigungen infolge von in den aktiven e-Mail-Inhalten enthaltenen Viren etc. resultieren, wesentlich verringern. Der wirtschaftliche Nutzen der erfindungsgemäßen Anordnung ist insoweit nicht nur für den Einzelnen, sondern für die gesamte Volkswirtschaft außerordentlich groß.

[0020] Vorteilhafte vorrichtungstechnische Maßnahmen sind in den Ansprüchen 15 bis 18 beschrieben.

[0021] Schließlich liegt es noch im Rahmen der Erfindung entsprechend Anspruch 19, ein Verfahren bzw. eine Anordnung gemäß der Erfindung zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen von aktiven e-Mail-Inhalten zu benutzen. Die Verwendung von erfindungsgemäßem Verfahren bzw. erfindungsgemäßer Anordnung insbesondere bei der Übertragung von e-Mails führt zu dem ausgesprochen großen Vorteil, die zu übertragende bzw. zu übermittelnde Datenmenge beträchtlich sicherer zumachen. In jedem Fall wird der Benutzer und damit Empfänger einer e-Mail auf einfache Weise davon (zum Beispiel von dem Provider) in Kenntnis gesetzt, ob eine e-Mail aktive e-Mail-Inhalte aufweist, die unter Umständen zu Schäden oder Beeinträchtigungen innerhalb seines Systems führen können.

Ausführungsbeispiel

[0022] Weitere Vorteile, Merkmale und Einzelheiten der Erfindung ergeben sich aus der nachfolgenden Beschreibung einiger bevorzugter Ausführungsformen und eines Beispiels der Erfindung sowie anhand der Zeichnungen. Hierbei zeigen:

[0023] **Fig.** 1 eine schematische Darstellung einer Ausführungsform eines erfindungsgemäß ausgebildeten Verfahrens zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen elektronischer Medien, und

[0024] **Fig.** 2 eine schematische Darstellung der Ausführungsform des erfindungsgemäß ausgebildeten Verfahrens der **Fig.** 1 in detaillierter Darstellung.

[0025] Das Verfahren und die Anordnung nach der Erfindung eignen sich insbesondere zum Blockieren von Daten und/oder Informationen und/oder Signalen, die einem Benutzer mittels einer e-Mail zugesendet wird, welches über ein elektronisches Datennetz, insbesondere über vorzugsweise das Internet, oder sonstiges Intranet, übertragen wird. Auf ausgesprochen vorteilhafte Weise dient das Verfahren und die Anordnung nach der Erfindung zur Verhinderung einer unwillkürlichen und unbeabsichtigten Ausführung aktiver e-Mail-Inhalte, zum Beispiel von Programmen, Skripten und/oder Virenprogrammen.

[0026] In der **Fig.** 1 ist das erfindungsgemäße Verfahren schematisch dargestellt. Demnach werden an den Benutzer gesendete Daten, Datenzellen oder Datenpakete und/oder Informationen und/oder Signale von einer Datenverarbeitungseinrichtung, insbesondere einem Server, beispielsweise einem Mail-Server, aus dem elektronischen Datennetz empfangen und anschließend in der Datenverarbeitungseinrichtung gespeichert.

[0027] Sodann werden die gespeicherten Daten und/oder Informationen und/oder Signale in deren einzelne

Bestandteile zerlegt. So besteht jede e-Mail aus einer einzelnen physikalischen Datei, die wiederum aus mehreren logischen Abschnitten bzw. einzelnen Dateien, sogenannten Dateianhängen, zusammengesetzt ist. In der Tab. 1 ist beispielhaft eine e-Mail im MIME-Format ohne Adress- und Mailroutingbestandteile dargestellt.

MIME-Version: 1.0 Content-Type: multipart/mixed; boundary=PART.103.saturn.705940.1	MIME-HEADER
--PART.103.saturn.705940.1 Content-type: text/richtext Content-Transfer-Encoding: quoted-printable	MIME-PART-HEADER
Deine Frage: Wie funktioniert MetaMail ? m=F6chte ich im folgenden beantworten. In der folgenden Referenz findest Du eine Graphik zur PP-Struktur.	PART-CONTENT
--PART.103.saturn.705940.1 Content-type: audio/basic Content-Description: Nutzung von MetaMail Content-Transfer-Encoding: base64	MIME-PART-HEADER

/n/+/n7++/98//5+fn7+/n7/fn/+fv7+fn79/3/9fv/ /f/7+fP5+fvt9/v7...	PART-CONTENT
--PART.103.saturn.705940.1 Content-Type: application/msword Content-Transfer-Encoding: base64 Content-Disposition: attachment; filename="testtext.doc"	MIME-PART-HEADER
0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAA AABAAAAIQAAAAAAAAAAEAAAIwAAAAEAAAD+////AAAAACAAAAD/////// ////////////////////////////////...	PART-CONTENT
--PART.103.saturn.705940.1-	MIME_FOOTER

[0028] Die Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale werden im Anschluss daran auf aktiven Inhalt überprüft. Dabei werden die Bestandteile der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt ermittelt bzw. bestimmt.

[0029] Ohne im Einzelnen dargestellt zu sein, können die in Bestandteile zerlegten Daten und/oder Informationen und/oder Signale klassifiziert und in geeigneter Weise abgelegt bzw. zwischengespeichert werden.

[0030] Schließlich werden die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt auf der Datenverarbeitungseinrichtung, d.h. dem Server bzw. Mail-Server,

zum gezielten Abruf durch den Benutzer bereitgestellt.

[0031] Die einzelnen Bestandteile der e-Mail werden, wie in der **Fig.** 2 dargestellt ist, auf folgende Weise hinsichtlich deren aktiven Inhalt überprüft. Dementsprechend werden die einzelnen Bestandteile der e-Mail, soweit technisch möglich, in Formate konvertiert bzw. umgewandelt bzw. durch Formate ersetzt, welche vollkommen ungefährlich sind, d.h. keine aktiven, potentiell gefährlichen Inhalte tragen oder tragen können. Die Konvertierung bzw. Ersetzung kann dabei automatisch oder auf Anforderung erfolgen.

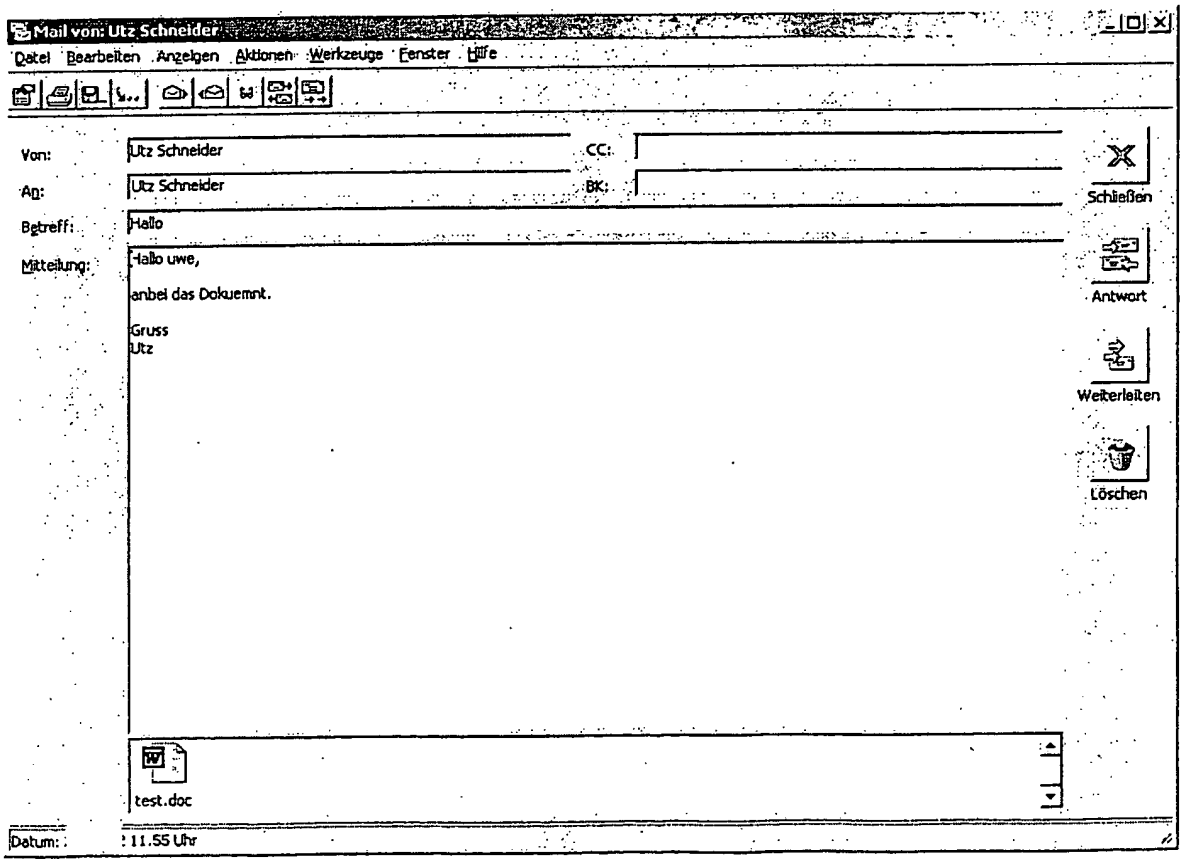
[0032] Zusätzlich werden Bestandteile der e-Mail erzeugt, welche eine Möglichkeit zum Erhalt der Bestandteile der e-Mail im Original offerieren. Für nicht konvertierbare Bestandteile der e-Mail oder Bestandteile mit aktiven, potentiell gefährlichen e-Mail-Inhalten werden ersatzweise neue Bestandteile erzeugt, die den Benutzer über das Vorhandensein dieser Bestandteile und deren Gefahrenpotential informieren sowie eine Möglichkeit zum Erhält einzelner Bestandteile der e-Mail oder sogar der gesamten e-Mail offerieren.

[0033] Zu diesem Zweck besteht die Möglichkeit, ein Link auf einer Website oder einem FTP-Server, auf welcher bzw. in welchem die einzelnen Bestandteile der e-Mail und die gesamte e-Mail zum Herunterladen bereitstehen, über das Internet oder sonstiges Intranet zu öffnen. Alternativ dazu ist es denkbar, die einzelnen Bestandteile der e-Mail oder die gesamte e-Mail im Original beim Provider anzufordern, indem diesem eine speziell vorbereitete e-Mail zurückgesendet wird, welche, ebenfalls automatisch oder auf Anforderung, beim Provider eine Versendung der einzelnen Bestandteile der e-Mail oder der gesamten e-Mail im Original an den Benutzer auslöst. Ein versehentliches oder automatisches Aktivieren von e-Mail-Inhalten mit Viren oder sonstigem Gefahrenpotential wird auf diese Weise einfach, zuverlässig und besonders kostengünstig verhindert.

[0034] Aus den konvertierten und neuen Bestandteilen wird schließlich eine neue e-Mail zusammengesetzt und anstelle der e-Mail im Original standardmäßig weiterverarbeitet. Diese lässt sich dann über herkömmliche e-Mail-Programme abrufen.

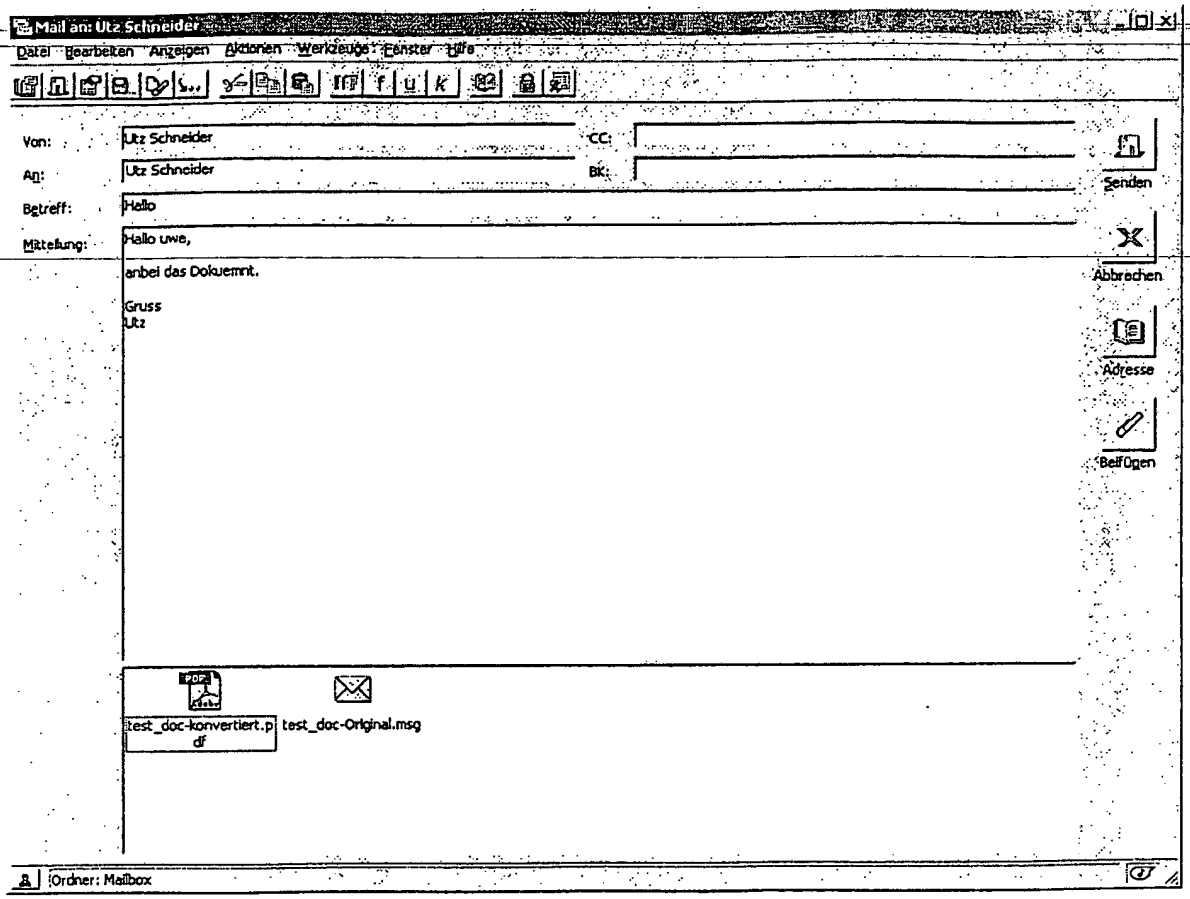
[0035] Nachfolgend wird das erfindungsgemäße Verfahren anhand eines Beispiels im konkreten Ablauf aus der Sicht des Benutzers näher erläutert:

Die nachfolgende Tab. 2 zeigt die Ansicht des Benutzers beim Empfang eines e-Mails mit einem herkömmlichen Dateianhang. Dabei ist ein Dateianhang in jedem Format, zum Beispiel im herkömmlichen MS-Office-Format, denkbar. Bei dem in der Tab. 2 dargestellten Dateianhang handelt es sich um die Word-Datei "test.doc".



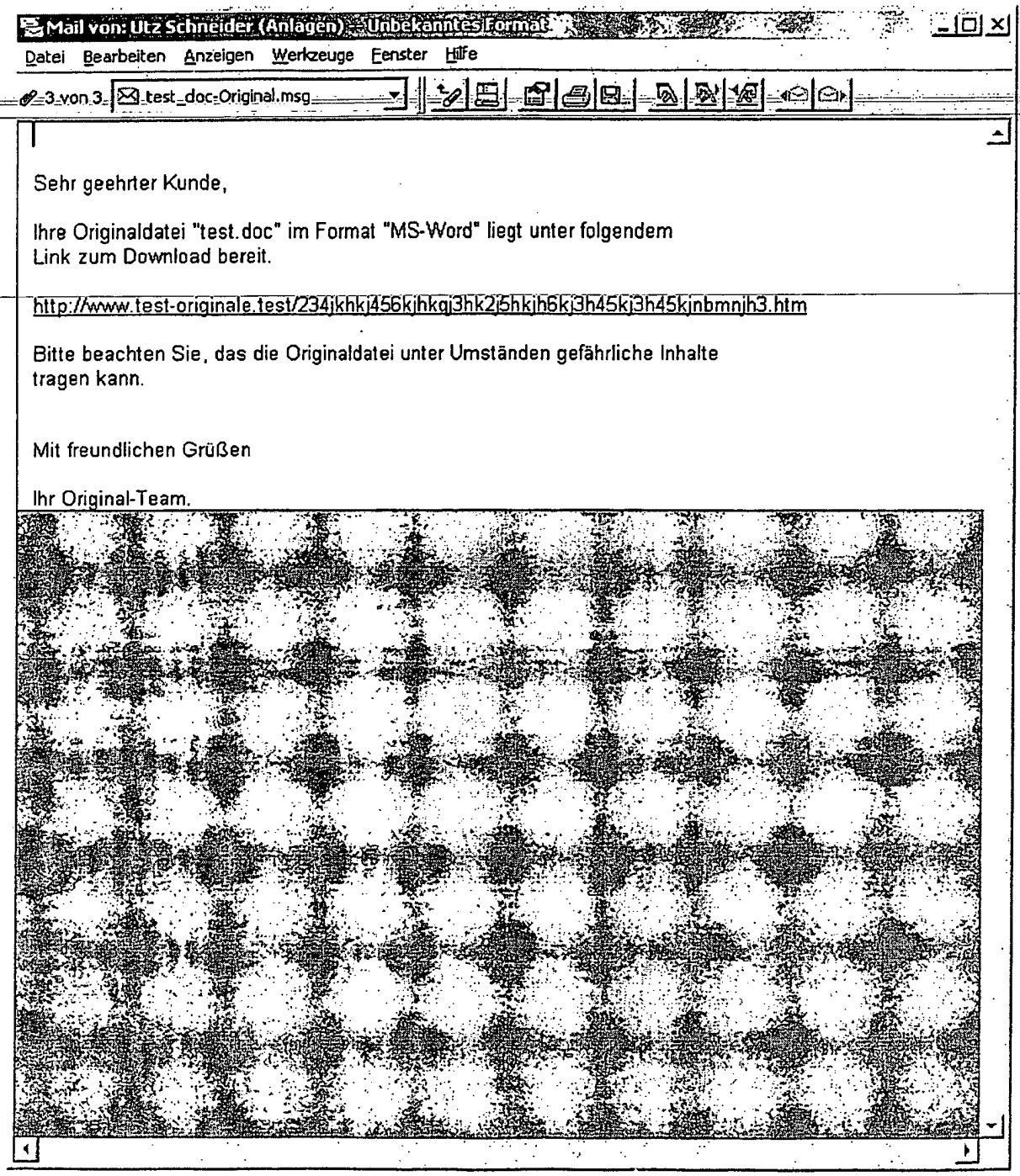
[0036] In Tab. 3 ist die Ansicht des Benutzers der e-Mail bei deren Empfang dargestellt, die zuvor einer Konvertierung unterzogen worden ist. Bestandteile in den Dateianhängen sind jetzt die in das PDF-Format konver-

tierte Word-Datei "test dockonvertiert.pdf", die sich mit einem gewöhnlichen PDF-Viewer lesen lässt, und die zusätzlich angefügte, im MSG-Format gehaltene Datei "test-doc-Original.msg", die eine Möglichkeit zum Erhalt des Originals offeriert. Für nicht konvertierbare Dateianhänge, wie zum Beispiel Programme im EXE-Format würde ausschließlich der Dateianhang "test doc-Original.msg" übermittelt werden.



[0037] Schließlich zeigt Tab. 3 alternativ den Inhalt des Dateianhangs "test_doc-Original.msg" zusammen mit einem Link zur Originaldatei, um es dem Benutzer zu ermöglichen, die e-Mail im Original über vorzugsweise das Internet, oder sonstiges Intranet, abzurufen. Alternativ dazu ließe sich auch der eigentliche Text der e-Mail um den Inhalt des Dateianhangs im MSG-Format erweitern, anstelle den Dateianhang in MSG-Format zu versenden.

[0038]



Die Erfindung ist nicht auf die dargestellte Ausführungsform des Verfahrens entsprechend den **Fig.** 1 und 2 und/oder der Tab. 1 bis 4 beschränkt. So ist es möglich, das Verfahren auch vom Benutzer selbst figurieren zu lassen. In diesem Zusammenhang wäre es beispielsweise denkbar, für jedes Postfach einer e-Mail individuell Sicherheitsrichtlinien, Konvertierungsoptionen und Zustellarten zu bestimmen.

Patentansprüche

1. Verfahren zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen elektronischer Medien, insbesondere von aktiven e-Mail-Inhalten, aus einem elektronischen Datennetz, insbesondere aus dem Internet oder sonstigem Intranet, umfassend folgende Schritte:
a) Empfangen der an den Benutzer gesendeten Daten und/oder Informationen und/oder Signale von einer Datenverarbeitungseinrichtung, insbesondere einem Server, aus dem elektronischen Datennetz,

b) Speichern der empfangenen Daten und/oder Informationen und/oder Signale aus Schritt a) in der Datenverarbeitungseinrichtung,
c) Zerlegen der gespeicherten Daten und/oder Informationen und/oder Signale aus Schritt b) in deren Bestandteile,
d) Überprüfen der Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale aus Schritt c) auf aktiven Inhalt,
e) Ermitteln der Bestandteile der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt, und
f) Bereitstellen der Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt aus Schritt d) und e) auf der Datenverarbeitungseinrichtung zum gezielten Abruf durch den Benutzer.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die gespeicherten Daten und/oder Informationen und/oder Signale in Schritt c) in deren kleinstmögliche Bestandteile zerlegt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale aus Schritt c) vor deren Überprüfung nach Schritt d) klassifiziert und (zwischen-) gespeichert werden.

4. Verfahren nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, dass die Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale aus Schritt c) bei deren Überprüfung nach Schritt d) wenigstens teilweise, vorzugsweise sämtlich, in Bestandteile ohne aktiven Inhalt konvertiert werden.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale automatisch in Bestandteile ohne aktiven Inhalt konvertiert werden.

6. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale auf Anforderung in Bestandteile ohne aktiven Inhalt konvertiert werden.

7. Verfahren nach den Ansprüchen 1 bis 6, dadurch gekennzeichnet, dass die nicht-konvertierbaren Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale mit aktivem Inhalt ermittelt und besonders gekennzeichnet werden.

8. Verfahren nach den Ansprüchen 1 bis 7, dadurch gekennzeichnet, dass die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt zusammen mit den Bestandteilen der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt auf der Datenverarbeitungseinrichtung zum Abruf durch den Benutzer bereitgestellt werden.

9. Verfahren nach den Ansprüchen 1 bis 7, dadurch gekennzeichnet, dass die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt getrennt von den Bestandteilen der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt auf der Datenverarbeitungseinrichtung zum Abruf durch den Benutzer bereitgestellt werden.

10. Verfahren nach den Ansprüchen 1 bis 9, dadurch gekennzeichnet, dass die auf der Datenverarbeitungseinrichtung bereitgestellten Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt von dem Benutzer unmittelbar abgerufen werden.

11. Verfahren nach den Ansprüchen 1 bis 9, dadurch gekennzeichnet, dass die auf der Datenverarbeitungseinrichtung bereitgestellten Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt von dem Benutzer unmittelbar abgerufen werden.

12. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt durch gesondertes Abrufen eines Links im elektronischen Datennetz auf der Datenverarbeitungseinrichtung zum Abruf durch den Benutzer bereitgestellt werden.

13. Verfahren nach Anspruch 11, dadurch gekennzeichnet, dass die Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt durch gesondertes Absenden einer Bestätigung zum Herunterladen über das elektronische Datennetz auf der Datenverarbeitungseinrichtung zum Abruf durch den Benutzer bereitgestellt werden.

14. Anordnung zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen elektronischer Medien, insbesondere von aktiven e-Mail-Inhalten, aus einem elektronischen Datennetz, insbesondere aus dem Internet oder sonstigem Intranet, nach einem der vorhergehenden Ansprüche, umfassend eine Einrichtung zum Empfangen der an den Benutzer gesendeten Daten und/oder Informationen und/oder Signale von einer Datenverarbeitungseinrichtung, insbesondere einem Server, aus dem elektronischen Datennetz, eine Einrichtung zum Speichern der empfangenen Daten und/oder Informationen und/oder Signale in der Datenverarbeitungseinrichtung, eine Einrichtung zum Zerlegen der gespeicherten Daten und/oder Informationen und/oder Signale in deren Bestandteile, eine Einrichtung zum Überprüfen der Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale auf aktiven Inhalt, eine Einrichtung zum Ermitteln der Bestandteile der Daten und/oder Informationen und/oder Signale mit aktivem Inhalt, und eine Einrichtung zum Bereitstellen der Bestandteile der Daten und/oder Informationen und/oder Signale ohne aktiven Inhalt und/oder mit aktivem Inhalt auf der Datenverarbeitungseinrichtung zum gezielten Abruf durch den Benutzer.

15. Anordnung nach Anspruch 14, gekennzeichnet durch eine Einrichtung zum Zerlegen der gespeicherten Daten und/oder Informationen und/oder Signale in deren kleinstmögliche Bestandteile.

16. Anordnung nach Anspruch 14 oder 15, gekennzeichnet durch eine Einrichtung zur Klassifizierung und (Zwischen-) Speicherung der Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale.

17. Anordnung nach einem der Ansprüche 14 bis 16, gekennzeichnet durch eine Einrichtung zum wenigstens teilweisen, vorzugsweise vollständigen, Konvertieren der Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale in Bestandteile ohne aktiven Inhalt.

18. Anordnung nach einem der Ansprüche 14 bis 17, gekennzeichnet durch eine Einrichtung zum Kennzeichnen der nichtkonvertierbaren Bestandteile der zerlegten Daten und/oder Informationen und/oder Signale mit aktivem Inhalt.

19. Verwendung des Verfahrens und der Vorrichtung nach einem der vorhergehenden Ansprüche zum Blockieren von an einen Benutzer gesendeten Daten und/oder Informationen und/oder Signalen von aktiven e-Mail-Inhalten.

Es folgen 2 Blatt Zeichnungen

Anhängende Zeichnungen

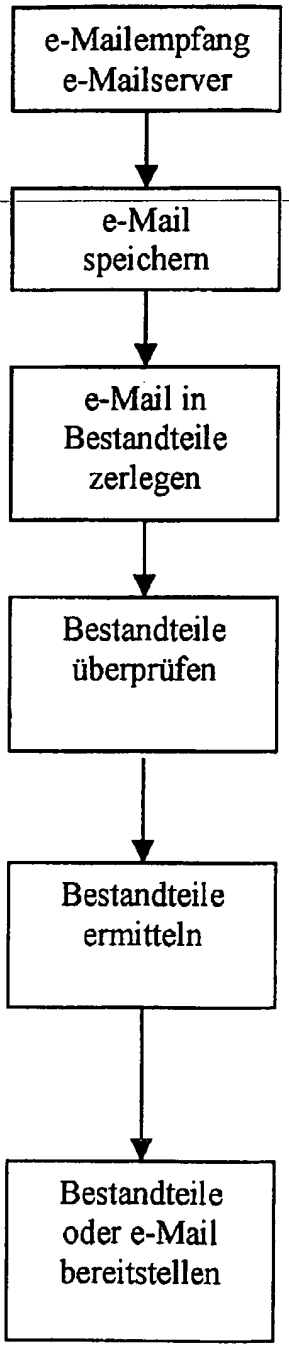


Fig.1

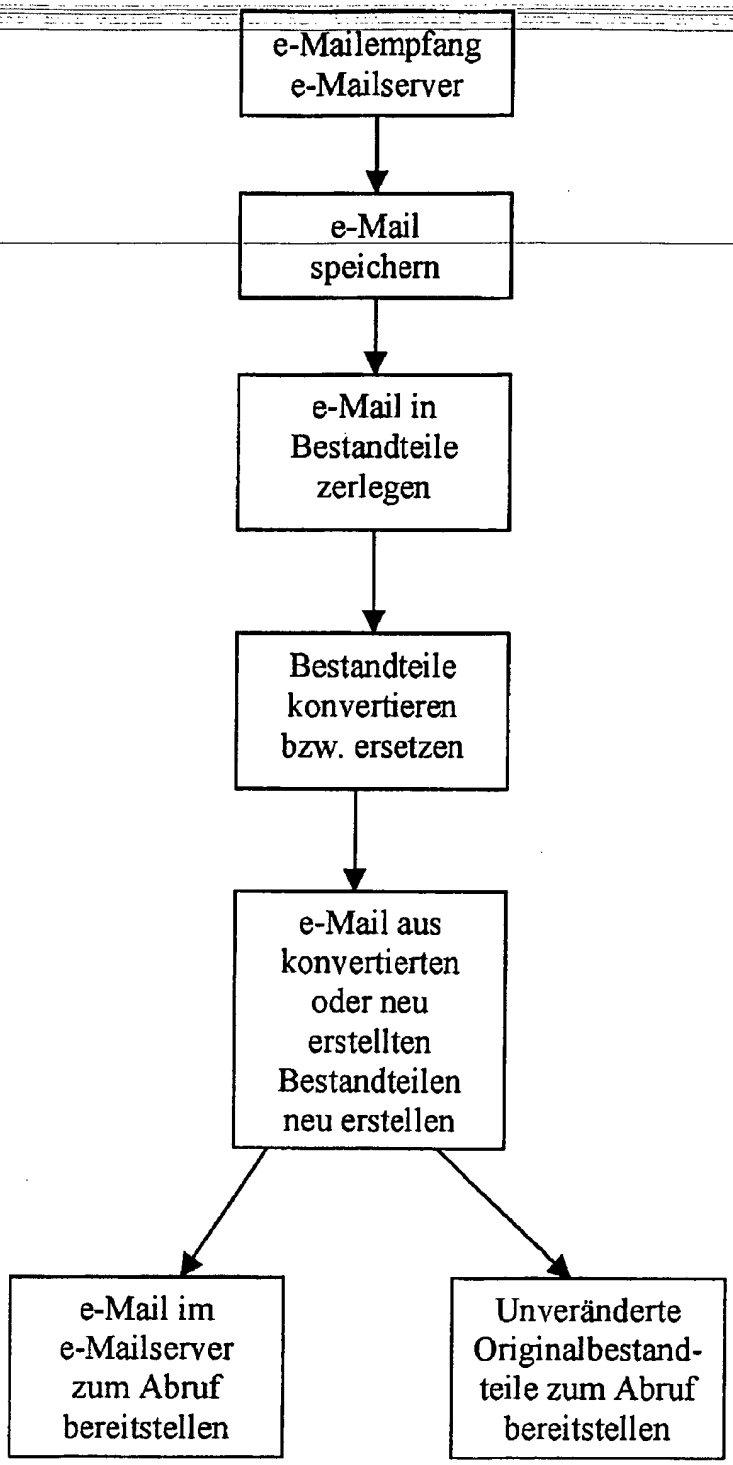

e-Mailempfang e-Mailserver
e-Mail speichern
e-Mail in Bestandteile zerlegen
Bestandteile konvertieren bzw. ersetzen
e-Mail aus konvertierten oder neu erstellten Bestandteilen neu erstellen
e-Mail im e-Mailserver zum Abruf bereitstellen
Unveränderte Originalbestand-teile zum Abruf bereitstellen

Fig.2